

Spring Conference of the Austrian Commission of Jurists

“Everything under Control?”, Weissenbach am Attersee, 21 May 2009

“Current Challenges for Data Protection in Europe”

Peter Hustinx

European Data Protection Supervisor

Ladies and gentlemen,

I would like to thank you, first of all, for inviting me to this annual spring conference about a very interesting subject that is very close to my heart: the fundamental right to privacy and data protection, and the growing tendency for public authorities to require access to personal data for an increasing range of public interests.

The subject of your conference is highly relevant, as the protection of personal data is also increasingly relevant. The respect for private life and the protection of personal data have been recognised as separate fundamental rights in Articles 7 and 8 of the EU Charter of fundamental rights. The Charter will become binding when the Lisbon Treaty is ratified. The right to the protection of personal data will be enhanced in the Lisbon Treaty in different ways.

This is a very important step in which a legal development of the last few decades in Europe will be confirmed. The right to data protection has been developed during that period as a system of rules and principles that allows a more structural approach to the issues of an Information Society. At the same time, our societies are now becoming increasingly dependent upon the widespread use of information and communication technologies, and this inevitably also leads to a massive processing of personal data in almost all fields of life.

In other words, while data protection as a *fundamental right* is *increasingly relevant*, it is also becoming a key challenge to ensure an *effective protection* of personal data

in practice. This sounds like a paradox, but fundamental rights are not intended for easy situations only.

Against this background, I would like to share with you some current challenges for data protection in Europe. As you will see, I am also convinced that there are major opportunities for the improvement of data protection ahead. An example already mentioned is the Lisbon Treaty, assuming that it is ratified by all Member States by the end of this year.

Relevance and Sensitivity

The increasing relevance of data protection has also led to an increasing political importance and sensitivity of various privacy issues. It is not exaggerated to say that privacy is increasingly a “hot” subject. This is clearly visible in the current revision of the e-Privacy Directive, which is a part of a larger Telecom Package. It is also visible in a growing interest for other online privacy issues, particularly online marketing, where different Commissioners are competing for responsibility in setting the agenda for future initiatives.

However, an increasing relevance and sensitivity are also visible in a growing interest for the future of Directive 95/46/EC, the main data protection framework adopted in 1995, which was the subject of a first conference this week organised by the European Commission to take stock of current views and developments.

The same is visible in the EU Justice and Home Affairs area and in the preparation of the policy programme for the next five years, usually referred to as the “Stockholm Programme” to be adopted under Swedish presidency later this year. It is also visible in a wider context, most of all in the transatlantic arena, where crucial developments might well take place in the next couple of years.

Finally, it is visible in different member states, such as in Germany, where citizens and consumers are becoming more engaged in privacy issues. It is also visible where privacy and data protection authorities are becoming more active and assertive in enforcement. And last but not least, where courts at all levels, both national and

European, are increasingly dealing with privacy issues and are delivering judgments that could further engage the legal profession.

Privacy Online

Let me now focus on some of these areas, starting with the revision of the e-Privacy Directive and other online privacy issues.

The revision of the e-Privacy Directive is a part of a larger package of measures aimed at the telecommunications sector, an area of great importance for economic recovery. In spite of the urgency of these measures, the package is currently blocked between Council and Parliament on one point, which is basically a conflict between the protection of privacy online and the protection of intellectual property rights against illegal downloading. Some countries take measures allowing service providers to monitor the use of the Internet and resulting in a denial of access for users who are suspected of repeated offences. The question is to which extent such measures should be permissible in the future.

If the revised e-Privacy Directive is finally adopted, it will bring some interesting new elements in the data protection landscape. One of them is the mandatory notification of security breaches. These breaches are an increasing problem - more visible in some member states, such as the UK, with more than 300 reported breaches a year - but not only there, in fact some scandals have recently occurred in Germany. It seems to me that we are dealing with a structural problem that is likely to undermine public trust and confidence in our increasingly "e-dependent" societies, if we do not take effective action. In my view there is a need for better data governance and more accountability. The top level of organisations should be involved and be held accountable for privacy compliance and better security arrangements in practice.

In principle, there are two main options. One option is that Article 17 of the current Data Protection Directive - which requires "appropriate technical and organisational measures to protect personal data against unlawful processing" - is interpreted in the sense that it also requires adequate arrangements for internal data governance. The other option is the introduction of compulsory security breach notifications, which

might lead to the same result from the "back end". One of the main benefits is that it would create a strong incentive for better security measures in organisations. The main challenge now is to develop a model for security breach notification that will be most effective in practice, i.e. with the right definitions of "security breach" and the right standards for notification to both users and authorities. Initially, the scope of the obligation will be limited to the e-Privacy Directive, but there is no reason not to go further and make it a general feature of data protection law, and I think this is exactly what should happen.

Other relevant issues in the online environment are data retention by search engines, the growing use of social networks, and data gathering for online advertising. There is an obvious link between those three issues, which makes them highly strategic. It so happens that online advertising is currently the main business model on the web and a great incentive for providers of search engines and social networks. The more data on users are available, the more targeted the advertising can be, and the more profitable the model becomes. This is why the Article 29 Working Party has recently given special attention to search engines and social networks, and is likely to come up with guidelines for online advertising as well.

Earlier this month, the European Commission published a Recommendation on the use of Radio Frequency Identification (RFID) as a cornerstone of the "Internet of Things". In the near future, more and more objects in our daily lives are expected to be online and exchange data about their users. In view of these developments, it is crucial that we interact with technology in such a way that privacy considerations can be built in at an early stage ("Privacy by Design"). This is a promising approach that is also on the agenda of your conference.

The Future of Directive 95/46/EC

This brings me to the future of the main Community framework for data protection, laid down in Directive 95/46/EC. Until recently the clear emphasis was on a better implementation of the existing legal framework. This involved different action lines, including a clarification of certain concepts and principles. The Article 29 Working Party has published an opinion on the concept of "personal data", and is now looking

into the concepts of "controller" and "processor". The first of these concepts is a crucial element for the scope of data protection safeguards. The latter two play a key role in the allocation of responsibility for compliance with data protection rules and principles, and they also have important consequences for the applicable national law. This explains why they have been selected for analysis.

The possibility of infringement procedures against different Member States was another action line. This is now also a reality in the pending case before the European Court of Justice against Germany about the principle of "independent supervision". Article 28 of the Directive requires that supervisory authorities should "act with complete independence" in exercising their functions. This principle is also visible in the Charter of fundamental rights and the Lisbon Treaty. A decision of the Court in the German case may therefore have far reaching consequences for institutional arrangements, both in Germany and in other Member States.

I fully share the emphasis on a better implementation of the existing legal framework. At the same time, I have expressed the view, already some years ago, that a revision of Directive 95/46/EC is unavoidable. The main argument is that revision is necessary to ensure that the Directive will remain effective in a changing world. This approach requires good preparation and careful planning. It is interesting in this context that the Commission is now also moving in this direction. Just this week, it organised a first conference in Brussels to take stock of current views and developments. Soon, the Commission will also launch a wide public consultation on the future of the existing legal framework.

If we think about different options available at this point, it is fair to assume that any revision will take a number of years. In fact, I expect that the new Commission will need at least two years to digest the results of the public consultation and to draw its own conclusions. In other words, I would not be surprised if any proposal from the Commission would not be submitted before 2012. The discussion about the review of the Directive in Parliament and Council could easily take another two or three years and thus last until 2015.

This timeframe has two important consequences. First, the emphasis on a better implementation of existing provisions should be maintained in the meantime. It would be highly unfortunate if we were to reduce our efforts to ensure compliance with existing data protection rules in a situation where the relevance of these rules is beyond any doubt. Secondly, the debate about a revision should focus on the needs for effective protection in 2015 and beyond. This will require creative solutions to ensure continued effectiveness of data protection in a changing environment. One way to deal with this challenge is to focus more on outcome than on detailed procedures, and to emphasize the responsibility of controllers for adequate compliance and to make them more accountable. In this context, data protection authorities would also need to have adequate powers and sufficient resources to execute their tasks independently and effectively, including the possibility to set their own priorities.

However, it may well be that a part of the answer lies in additional measures with a more limited scope, which could interact with the general provisions of the Data Protection Directive. This model already exists in the e-Privacy Directive. It might also be useful for the introduction of compulsory data breach notifications in a more horizontal fashion. The same is true for the possible need for specific measures on RFID or – to mention yet another area – for the possible introduction of measures on privacy relevant services, such as privacy auditing, privacy certification and similar activities.

In other words, if we think about the architecture of data protection law, we should not assume that one approach will be sufficient to fit all needs and circumstances. Let me also make the point that competition – both between responsible controllers and between service providers of different categories – may also be an interesting element of the data protection governance landscape in the future.

Privacy and Law Enforcement

Other important issues arise in the context of law enforcement. Special powers in this field always require a careful evaluation to ensure a good balance between the needs of law enforcement and the needs of privacy and data protection. The legal framework for this evaluation has been laid down in Article 8 of the European Convention on

Human Rights. Any interference with the right to respect for private life should have a clear and precise legal basis. Any such measure should be *necessary* in a democratic society for a pressing social need, and should be accompanied by adequate safeguards against possible abuse.

The principle of *proportionality* has been illustrated recently in the decision of the European Court of Human Rights in the Marper case. Although this case was, strictly speaking, only about the retention of DNA data concerning suspects of crime, the Court's message can easily be understood in a much wider sense. In fact, it would be good, if we would apply it not only to new measures, but also to evaluate whether previously adopted measures still satisfy the conditions of lawfulness under Article 8. This also applies to Directive 2006/24/EC on the retention of communication data which will be evaluated soon.

New issues arise in the context of information systems for the exchange of law enforcement data between Member States. Some of these systems already exist, such as the Schengen Information System (SIS I), which is being revised and extended into a larger system for more participating countries and more functionalities (SIS II). Other systems are either in the course of development or expected in the near future. It would be good in my view if the Stockholm Programme would provide a clear policy framework for the development of such systems. Part of this framework should be that the principle of "Privacy by Design" applies to their development. There is also a clear need for a long term vision, as initiatives in this field have too often been driven by ad hoc considerations.

More specifically as to data protection, it should be noted that Council framework Decision 2008/977/JHA has laid down common rules for data protection in the context of police and judicial cooperation in criminal matters. However, the scope of these rules is unsatisfactory, as they only apply to transfers of data across national borders and not to purely domestic data, although the distinction between these categories is increasingly difficult in practice. Another problem is that the new rules are not consistent with Directive 95/46/EC. The exchange of data between private sector and law enforcement will therefore also lead to increasing difficulties. This

means that both the scope and the content of the new rules should be improved in the near future.

Global Privacy

The need for global safeguards is also increasing, as more and more activities have a global dimension or are becoming interconnected.

The scope of European data protection law is not limited to the Member States of the European Union, as it applies to *all* processing of personal data in the *context* of an *establishment* of the controller in an EU Member State. This means that outsourcing of activities to a third country is subject to European data protection law. However, transfer of data to third countries is also subject to safeguards, regardless of whether the responsibility remains at the EU controller. This system of safeguards is based on a distinction between third countries with or without an adequate level of protection.

More and more countries around the world – in North-America, Latin America, and the Asia-Pacific region – have some kind of data protection law. All in all, some fifty or sixty countries around the world, including some recent initiatives in Africa, are in this category. There is indeed also a growing convergence between privacy safeguards in different regions of the world.

Different initiatives have been taken to come to global privacy standards to simplify international data flows. One of those initiatives – sponsored by the International Conference of Data Protection and Privacy Commissioners – will probably lead to the presentation of a Joint Proposal for International Standards at the 31st International Conference in November 2009 in Madrid. This proposal will show the feasibility of international standards as the basis for an International Convention to be concluded in due course.

In the interim period, the standards can also be useful as a framework for contractual and self-regulatory solutions in different sectors. The Article 29 Working Party has invested heavily in the development of “Binding Corporate Rules” as a promising tool for multi-national enterprises to ensure that their data processing activities around the

world comply with adequate standards. This should of course be taken into account in a possible revision of Directive 95/46/EC.

Some more focussed activities can also be expected in the transatlantic relationship in the coming years. The report of a High Level Contact Group of EU and US officials which was presented last year, has established a substantial overlap between European and US safeguards on privacy and data protection. If remaining problems are solved, it would be possible to work out a binding international agreement for the exchange of law enforcement information. One of the remaining serious problems is that US law does not provide for judicial review of decisions affecting non US citizens and that the Privacy Act also has a narrow scope. However, I would not be surprised, if these obstacles could be eliminated and substantial progress could be made within a few more years.

Lisbon Treaty

This brings me back to the Lisbon Treaty already mentioned in the beginning. If the Treaty would be finally ratified by all Member States and would enter into force early next year, this would have important consequences for data protection on at least two different levels.

At institutional level, the entry into force of the Lisbon Treaty will lead to the end of the pillar structure. One important consequence is that the Community method of decision making – involving both Council and European Parliament – will also apply for subjects of the current Third Pillar. This means that the Parliament will no longer be limited to an advisory role, but will be fully responsible in a co-decision procedure. This is an important safeguard for more balanced decision making and hopefully also for more balanced results.

However, the Lisbon Treaty will also have important consequences for the structure of EU data protection law. Data protection law has so far developed in an internal market perspective and is still rather invisible in the different treaties. Article 286 EC Treaty provides that Community instruments on data protection – such as Directive 95/46/EC – also apply to the Community institutions and bodies, and provides the

basis for independent supervision by the EDPS. Article 30 (1)(b) EU Treaty requires appropriate safeguards for data protection in the context of data exchange for police and judicial cooperation in criminal matters.

At the same time, data protection has emerged as a horizontal issue. This was clear from the ECJ decision in the *Rechnungshof* case, also known as *Österreichischer Rundfunk* in May 2003, the first decision on Directive 95/46/EC and strictly speaking only dealing with an issue in the Austrian public sector. However, the ECJ took this case to emphasize the wide scope of the Directive. This trend was recognised in Article 8 of the Charter of fundamental rights, which will become binding with the entry into force of the Lisbon Treaty.

The Lisbon Treaty will also introduce a horizontal legal basis for data protection in Article 16 of the Treaty on the functioning of the European Union (TFEU), among the general principles of European law. This article will provide a subjective right to data protection. It will have “direct effect”, which means that everyone can rely on it in court. Article 16 also contains a formal obligation to lay down rules for the protection of personal data, which will apply to the European institutions and bodies, but also to the Member States when acting under the scope of Union law.

This provision will not have any immediate effect for Directive 95/46/EC, which will continue to apply until it is amended or replaced by another instrument. But it will have consequences for the recently adopted framework in the Third Pillar, as this does not fully comply with the new requirements and will therefore have to be replaced or amended by an instrument adopted in co-decision.

In any case, the new legal basis will provide an opportunity for a complete rethinking of European data protection law. This may have consequences in all areas discussed today. A final and very important challenge is therefore how to use the potential for a better and more effective data protection in the future.